



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/004,132	10/23/2001	Alexander W. Whytock	9086.00	8040
26889 7590 04/06/2007 MICHAEL CHAN NCR CORPORATION 1700 SOUTH PATTERSON BLVD DAYTON, OH 45479-0001			EXAMINER TRUONG, LAN DAI T	
			ART UNIT 2152	PAPER NUMBER
SHORTENED STATUTORY PERIOD OF RESPONSE		MAIL DATE	DELIVERY MODE	
3 MONTHS		04/06/2007	PAPER	

**Please find below and/or attached an Office communication concerning this application or proceeding.**

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

**Office Action Summary**

Application No.

10/004,132

Applicant(s)

WHYTOCK, ALEXANDER W.

Examiner

Lan-Dai Thi Truong

Art Unit

2152

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 03 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 02 January 2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 20-24 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 20-24 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_

### DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 01/02/2007 has been entered.

2. This action is response to communications: application, filed on 10/23/2001; amendment filed 01/02/2007; Claims 1-24 are pending; claims 1-19 are canceled; claims 20-24 are added

3. The applicant's arguments filed on 01/02/2007 have fully considered but they are moot in view with new ground for rejections

### Claim rejections-35 USC § 112, first paragraph

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claims 20 and 23 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter as a reference to an algorithm and a reference to an encryption key which was not described in the

Art Unit: 2152

specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Because the specification fails to support new claims languages; therefore, they constitute a new matter

5. Claims 20 and 23 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter such as a reference to an algorithm and a reference to an encryption key which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention; corrections is requested

For examining purpose, the Office will interpret "a reference to an algorithm" as "algorithm (des-ecb)" disclosed in figure 7, and "a reference to an encryption key" as "Key 1" disclosed in figure 7.

### **Claim rejections-35 USC § 112, second paragraph**

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 20 and 23 recite the limitation "executing the instructions to direct how the decrypted data and the input data..." in (claim 20, line 8; claim 23, line 8). There is insufficient antecedent basis for this limitation in the claim; as Applicant's disclosures the input data is

Art Unit: 2152

decrypted, so the decryption produce should be decrypted input data rather than the decrypted data; correction is requested

7. Claims 20 and 23 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps. See MPEP § 2172.01. The omitted steps are: Applicant claims method for receiving a file containing numbers of elements such as input data, a reference to an algorithm, a reference to an encryption key, and instruction for making a new encryption key; As said in one of the limitation of the claim 1, (lines 6-7), the input data is decrypted by using the referenced algorithm and the referenced encryption key; Examiner does not clearly understand how the input data is still exist after it already decrypted without any step of caching/or copying the input data prior decrypting step (disclosed in claim 1, line 8); In Examiner's opinion, at least one step of copying/or caching the input data is missing prior step of "Executing the instructions to direct how the decrypted data and the input data are to operated on produce a new encryption key...;" correction is requested

### **Claim rejections-35 USC § 103**

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 20-24 are rejected under 35 U.S.C 103(a) as being un-patentable over Matyas, Jr. et al. (U.S. 7,010,689) in view of Matyas et al. (U.S. 5,142,578) in view of Rhelimi (U.S. 6,049,790)

**Regarding to claim 20:**

Matyas, Jr discloses the invention substantially as claimed, including a method, which can be implemented in a computer hardware or software code for deriving a new encryption key for use in an encrypting keypad module, the method comprising:

Using the referenced algorithm and the referenced encryption key to decrypt input data; making a new encryption key; executing the instructions to direct how the decrypted data and input data are to be operated on to produce a new encryption key: (Matyas discloses method for decrypting “the encrypted file encryption key” which shares functionality with “input data” as claimed by using “the personal key” which is equivalent to “the referenced encrypted key” as claimed to provide “a recovered file encryption key/the encryption key” which shares functionality with “the decrypted data” as claimed; then the encryption key/means recovered encryption key is encrypted again to produce “a new encrypted file encryption key” which shares functionality with “a new encryption key” as claimed; the well-known technique in the art for encrypting/decrypting a data should be involved by encryption algorithm and instructions, so Matyas’s system inherently includes the encryption algorithm and instructions: column 2, lines 1-14)

However, Matyas Jr does not disclose receiving a file containing input data, a reference to an algorithm, a reference to encryption key

In analogous art, Matyas discloses “an external key token” which shares functionality with “a file” as claimed including encrypted key, control information, algorithm, and instructions, see (column 10, lines 62-67; column 11, lines 1-67; column 12, lines 1-67; column 8, lines 5-55)

However Matyas Jr- Matyas does not explicitly disclose storing encryption key at the encrypting keypad module

In analogous art, Rhelimi discloses method for using encrypted key and encrypted algorithm those are stored in “a keypad processing unit” which shares functionality with “the encrypting keypad module” as claimed for encrypting input data from the keypad, see (figure 1 item 10 and 14; figure 2, item 14 and 30; column 3, lines 1-35)

Thus, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate Matyas’s ideas of including encrypted key control information, algorithm, and instructions in an external key token with Rhelimi’s ideas of using included encryption key, and algorithm in keypad to encrypt input data into Matyas Jr’s system in order to improve security for communication system, see (Matyas: column 4, lines 3-8, lines 44-48)

**Regarding to claims 21 and 23:**

Those claims are rejected under rationale of claim 20

**Regarding to claims 22 and 24:**

Although, Matyas, Jr-Matyas-Rhelimi does not explicitly disclose a structure comprising tagged commands and data; However Jr-Matyas discloses program code used could be Java; it

Art Unit: 2152

would have been obvious in the art that Java program code built on structure of tagged commands and data

The prior arts made of records and not relied upon are considered pertinent to applicant's disclosure. The following patents and publications are cited to further show the state of the art with respect to "Encrypting keypad module": 5745576; 4941176; 6578145; 5404403; EP1191423; 6598023; 6763313; 6802013;

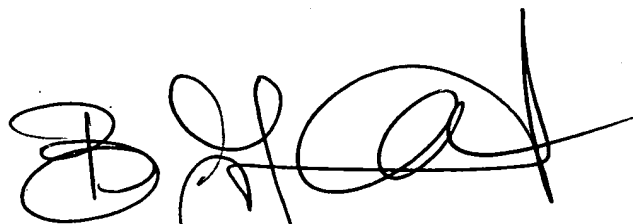
### **Conclusions**

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Lan-Dai Thi Truong whose telephone number is 571-272-7959. The examiner can normally be reached on Monday- Friday from 8:30am to 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Bunjob A. Jaroenchonwanit can be reached on 571-272-3913. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

04/01/2007



BUNJOB JAROENCHONWANIT  
SUPERVISORY PATENT EXAMINER